IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product embodied on a computer readable medium for controlling a mobile data processing device to update malware definition data for a malware scanner of said mobile data processing device, said computer program product comprising:

(i) link establishing code operable to establish a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) update receiving code operable to receive malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) malware definition updating code operable to update malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

2. (Original) A computer program product as claimed in claim 1, wherein said mobile data processing device is a mobile telephone.

3. (Original) A computer program product as claimed in claim 1, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

4. (Cancelled)

5. (Original) A computer program product as claimed in claim 1, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

6. (Original) A computer program product as claimed in claim 1, wherein said data channel is also used for passing text messages.

7. (Original) A computer program product as claimed in claim 6, wherein said text messages are SMS messages.

8. (Currently Amended) A computer program product as claimed in claim 1, wherein said step of ~~transferring~~receiving malware definition updating data is initiated from a source of said malware definition updating data.

9. (Original) A computer program product as claimed in claim 1, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

10. (Currently Amended) A computer program product embodied on a computer readable medium for controlling a computer to initiate updating of malware definition data for a malware scanner of a mobile data processing device, said computer program product comprising:

(i) link establishing code operable to establish a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) update sending code operable to send malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing

device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

11. (Original) A computer program product as claimed in claim 10, wherein said mobile data processing device is a mobile telephone.

12. (Original) A computer program product as claimed in claim 10, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

13. (Cancelled)

14. (Original) A computer program product as claimed in claim 10, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

15. (Original) A computer program product as claimed in claim 10, wherein said data channel is also used for passing text messages.

16. (Original) A computer program product as claimed in claim 15, wherein said text

messages are SMS messages.

17. (Original) A computer program product as claimed in claim 10, wherein transfer of malware definition updating data is initiated from a source of said malware definition updating data.

18. (Original) A computer program product as claimed in claim 10, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

19. (Currently Amended) A method of updating malware definition data for a malware scanner of a mobile data processing device, said method comprising the steps of:

(i) establishing a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) receiving malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) updating malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

20. (Original) A method as claimed in claim 19, wherein said mobile data processing device is a mobile telephone.

21. (Original) A method as claimed in claim 19, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

22. (Cancelled)

23. (Original) A method as claimed in claim 19, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

24. (Original) A method as claimed in claim 19, wherein said data channel is also used for passing text messages.

25. (Original) A method as claimed in claim 24, wherein said text messages are SMS messages.

26. (Original) A method as claimed in claim 19, wherein transfer of said malware definition updating data is initiated from a source of said malware definition updating data.

27. (Original) A method as claimed in claim 19, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

28. (Currently Amended) A method of updating malware definition data for a malware scanner of a mobile data processing device, said method comprising the steps of:

(i) establishing a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) sending malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

29. (Original) A method as claimed in claim 28, wherein said mobile data processing device is a mobile telephone.

30. (Original) A method as claimed in claim 28, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

31. (Cancelled)

32. (Original) A method as claimed in claim 28, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

33. (Original) A method as claimed in claim 28, wherein said data channel is also used for passing text messages.

34. (Original) A method as claimed in claim 33, wherein said text messages are SMS messages.

35. (Original) A method as claimed in claim 28, wherein transfer of said malware definition updating data is initiated from a source of said malware definition updating data.

36. (Original) A method as claimed in claim 2, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

37. (Currently Amended) Apparatus for controlling a mobile data processing device to update malware definition data for a malware scanner of said mobile data processing device, said apparatus comprising:

(i) link establishing logic operable to establish a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) update receiving logic operable to receive malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) malware definition updating logic operable to update malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition

updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

38. (Original) Apparatus as claimed in claim 37, wherein said mobile data processing device is a mobile telephone.

39. (Original) Apparatus as claimed in claim 37, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

40. (Cancelled)

41. (Original) Apparatus as claimed in claim 37, wherein said public wireless

telephone network is one of a CDMA network and a GSM network.

42. (Original) Apparatus as claimed in claim 37, wherein said data channel is also used for passing text messages.

43. (Original) Apparatus as claimed in claim 42, wherein said text messages are SMS messages.

44. (Original) Apparatus as claimed in claim 37, wherein said step of transferring is initiated from a source of said malware definition updating data.

45. (Original) Apparatus as claimed in claim 37, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

46. (Currently Amended) Apparatus for controlling a computer to initiate updating of malware definition data for a malware scanner of a mobile data processing device, said apparatus comprising:

(i) link establishing logic operable to establish a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) update sending logic operable to send malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition

updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

47. (Original) Apparatus as claimed in claim 46, wherein said mobile data processing device is a mobile telephone.

48. (Original) Apparatus as claimed in claim 46, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

49. (Cancelled)

50. (Original) Apparatus as claimed in claim 46, wherein said public wireless

telephone network is one of a CDMA network and a GSM network.

51. (Original) Apparatus as claimed in claim 46, wherein said data channel is also used for passing text messages.

52. (Original) Apparatus as claimed in claim 51, wherein said text messages are SMS messages.

53. (Original) Apparatus as claimed in claim 46, wherein transfer of malware definition updating data is initiated from a source of said malware definition updating data.

54. (Original) Apparatus as claimed in claim 46, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.